Innenausschuss
A-Drs 16(4)560 C

**GESELLSCHAFT FÜR DATENSCHUTZ
UND DATENSICHERUNG e.V.**

S t e l l u n g n a h m e

a) zu dem *Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften*
(BT-Drucksache 16/12011)

sowie zu den Anträgen

b) *Datenschutz-Audit-Verfahren und Datenschutz-Gütesiegel einheitlich regeln*
(BT-Drucksache 16/1169)

und

c) *Datenschutzaudit umsetzen – Gütesiegel stärkt Bürgerechte und schafft Akzeptanz für wirtschaftliche Innovation*
(BT-Drucksache 16/1499)

erstellt von

**Prof. Peter Gola,
Vorstandsvorsitzender der GDD e.V.**

Gesellschaft für Datenschutz
und Datensicherung e.V.
Pariser Str. 37 · 53117 Bonn
Tel.: 0228/69 43 13 · Fax: 0228/69 56 38
Internet: www.gdd.de · E-Mail: info@gdd.de

A. Zum Entwurf eines Datenschutzauditgesetzes
- zugleich zu den Anträgen b) und c) -

I. Grundsätzliches

Das in der Begründung zum Gesetzentwurf des DSAG formulierte Ziel, mit einem Datenschutzgütesiegel Aufwendungen von Unternehmen für besondere Aufwendungen zum Datenschutz zu honorieren und hierfür Marktanreize zu setzen wird grundsätzlich begrüßt. Allerdings ist festzustellen, dass auch der nunmehr vorliegende Entwurf nicht geeignet ist, das Ziel der Schaffung eines unbürokratischen Datenschutzaudits zu erreichen.

Positiv hervorzuheben ist, dass die Gesamtorganisation des Datenschutzes im Unternehmen bei einer Auditierung dadurch berücksichtigt wird, dass die organisatorische Stellung des Beauftragten für den Datenschutz separater Prüfungspunkt ist. Dies kann zur Stärkung der Position des Beauftragten für den Datenschutz beitragen (zur Einbeziehung des Datenschutzbeauftragten in das Auditverfahren vgl. die Ausführungen zu § 3 DSAG-E).

Bedauerlich ist allerdings, dass mit dem Gesetzentwurf keine klaren Prüfungsmaßstäbe vorgelegt wurden, sondern diese durch unterschiedliche Gremien (per Rechtsverordnung durch das BMI bzw. per Richtlinien durch den Datenschutzauditausschuss) erst noch zu entwickeln sind. Durch diese Ausgestaltung wird sich die Umsetzung des Auditgesetzes weiter verzögern; im Übrigen bestehen Zweifel an der Bestimmtheit eines solchen Gesetzestextes

Zu § 1 DSAG-E

Gegenstand eines Datenschutzaudits sollen verantwortliche Stellen hinsichtlich des Datenschutzkonzepts oder bei Anbietern von Datenverarbeitungsanlagen und Programmen die angebotenen informationstechnischen Einrichtungen sein.

Die Vorschrift greift damit den Anwendungsbereich des § 9a BDSG auf. Bei der gesetzlichen Konkretisierung wäre es jedoch sinnvoll, den Anwendungsbereich einer Zertifizierung auf Verfahren, Dienstleistungen und informationstechnische Produkte

zu beschränken. Nur in diesen Bereichen bestehen Anreize durch besondere Datenschutzanstrengungen, Erwerbsvorteile zu erlangen.

Zudem ist nicht nachvollziehbar, warum öffentliche Stellen (des Bundes) nicht zu den Normadressaten des DSAG gehören sollen. Auch hier kann eine Auditierung durchaus Mehrwerte mit sich bringen.

Zu § 3 DSAG-E (Kontrollen)

Die von den zugelassenen Kontrollstellen durchgeführte Prüfung und Zertifizierung ist von dieser Vorschrift auf eine dynamische und risikoadäquate Überprüfung angelegt. Dies verhindert, dass lediglich punktuell Datenschutzkonzepte und informationstechnische Einrichtungen auditiert werden. Da die entsprechenden Verfahren, Produkte und Dienstleistungen sich einem ständigem, zum Teil informationstechnisch bedingten Wandel unterstehen, ist zur Vertrauenswürdigkeit des Gütesiegels auch eine risikoadäquate Kontrolle angezeigt. Begrüßt wird ebenfalls, dass der betriebliche Datenschutzbeauftragte in die Durchführung der Kontrollen einzubeziehen ist. Dies wird in seiner BDSG angelegten Stellung als Compliance-Organ zum Datenschutz gerecht.

Zu § 4 DSAG-E (Zulassung der Kontrollstelle)

Die Kontrollstellen werden als Kern des Kontrollsystems angesehen. Insofern ist die über § 4 DSAG-E angestrebte hohe Qualifizierung der Stellen grundsätzlich zu begrüßen.

Die Anforderungen an die Zulassung einer Kontrollstelle sollten hinreichend bestimmt sein. Dies ist zumindest hinsichtlich der Anforderung einer Akkreditierung nach Abs. 1 Nr. 2 DSAG-E nicht der Fall, da die Vorgaben eine Akkreditierung nicht spezifiziert werden.

Zu § 6 DSAG-E (Pflichten der Kontrollstelle)

Im Hinblick auf die Akzeptanz des Datenschutzaudits und der Kontrollstellen sollte § 5 Abs. 3 DSAG-E überprüft werden. Durch die Vorschrift würden der Kontrollstelle

weitreichende Informationspflichten im Hinblick auf Unregelmäßigkeiten oder Verstöße auferlegt. Die Pflicht soll selbst dann eingreifen, wenn Verstöße oder Unregelmäßigkeiten bekannt werden, die bei einer verantwortlichen Stellen liegen, die nicht Auftraggeber der Kontrollstelle ist. Es sollte der Eindruck vermieden werden, die Kontrollstellen hätten den Auftrag, „Ermittlungen“ in Bezug auf Datenschutzverstöße durchzuführen.

Zu § 7 DSAG-E (Pflichten der zuständigen Behörde)

Nach dieser Regelung soll eine „zuständige Behörde“ des Landes soll die Kontrollstellen überwachen.

Unklar bleibt, wer zuständige Behörde eines Landes ist. Die Wahl einer offenen Formulierung ist zwar nachvollziehbar. Andererseits birgt sie die Gefahr, dass neben den bestehenden Datenschutzaufsichtsbehörden für die Kontrolle im nicht öffentlichen Bereich nach § 38 BDSG je nach Landesrecht weitere Zuständigkeiten geschaffen werden, was eine einheitliche Anwendung des Datenschutzrechts abträglich sein könnte.

Weiterhin bleibt offen, worauf sich die Überwachung der Kontrollstelle durch die zuständige Behörde exakt beziehen soll. Fraglich ist insofern, ob sich die Aufsicht nur auf „formale“ Aspekte der Kontrolltätigkeit beziehen soll oder ob auch eine inhaltliche Überprüfung der Tätigkeit möglich sein soll. Hier wäre eine Klarstellung wünschenswert.

Zu § 11 und 12 DSAG-E (Datenschutzauditausschuss)

Die Einrichtung eines Datenschutzauditausschusses ist grundsätzlich zu begrüßen. Im Hinblick auf die zügige Umsetzung des DSAG ist allerdings fraglich, wie lange es dauert, bis ein solcher Ausschuss gebildet ist bzw. bis wann er entsprechende Prüfkataloge entwickelt hat.

Die paritätische Besetzung des Datenschutzauditausschusses ist grundsätzlich zu begrüßen. Unverständlich bleibt allerdings § 12 Abs. 1 Nr. 4 DSAG-E, wonach ganz allgemein „zwei Vertreter der Verwaltung der Länder“ einbezogen werden sollen. Die Aufsichtsbehörden der Länder werden bereits nach § 12 Abs. 1 Nr. 5 DSAG-E be-

rücksichtigt. Für die Einberufung von Vertretern der allgemeinen Landesverwaltung besteht kein Anlass. Soweit über § 12 Abs. 1 Nr. 4 DSAG-E spezielle DSAG-Behörden (vgl. dazu bereits oben zu § 7 DSAG-E) erfasst werden sollen, sollte eine entsprechende Klarstellung erfolgen.

Mit Blick auf die Vertreter von Unternehmen und deren Verbände wird in der Gesetzesbegründung darauf hingewiesen, dass das Vorschlagsrecht bei den Bundesdachverbänden der Wirtschaft liegen soll. Sinnvollerweise sollten in diesem Zusammenhang auch Fachverbände, die die Wirtschaft in Datenschutzfragen beraten, berücksichtigt werden. Die Fachverbände bündeln nicht nur die Kompetenzen im Bereich des Datenschutzes, sie haben auch einen besonderen Bezug zur betrieblichen Praxis.

Zu § 16 DSAG-E (Verordnungsermächtigungen)

Die Umsetzung des Datenschutzaudits erfordert den Erlass diverser Rechtsverordnungen. Hier ist bereits fraglich, ob dies dem verfassungsrechtlich begründeten Parlamentsvorbehalt entspricht. Zudem ist festzustellen, dass die Verordnungsermächtigung in Widerspruch zu § 9a Satz 2 BDSG steht, wonach die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter durch besonderes Gesetz zu regeln sind.

B. Zum Entwurf zur Änderung des BDSG

1. Zu § 4f Abs. 3 BDSG-E (Betrieblicher Datenschutzbeauftragter)

Die Regelung eines Sonderkündigungsschutzes für Datenschutzbeauftragte wird begrüßt, da die Rechtsprechung bisher zumindest für teilamtliche Datenschutzbeauftragte aus dem Abberufungsschutz keinen besonderen Kündigungsschutz abgeleitet hat.

Neben der Gewährung eines Kündigungsschutzes bedarf es zusätzlich auch einer Stärkung der Rechtsposition des Datenschutzbeauftragten im Unternehmen. Viele Datenschutzskandale in jüngerer Vergangenheit sind dadurch gekennzeichnet, dass die betrieblichen Datenschutzbeauftragten über die geplante Datenverarbeitung nicht oder nicht rechtzeitig informiert worden sind. Hier sollte im Bundesdatenschutzgesetz eine unmittelbare Rechtsfolge an die Verletzung der Unterrichtungspflicht geknüpft werden. Zumindest für den Fall der gesetzlich geforderten Vorabkontrolle, die in besonders risikobehafteter Datenverarbeitung zur Anwendung kommt, sollte die mangelnde Konsultation des Datenschutzbeauftragten mit Sanktionen verbunden werden.

Unterstützt wird die Anregung des Bundesrates, die Anforderungen an die Fachkunde des Beauftragten für den Datenschutz zu konkretisieren. Die Praxis zeigt, dass auf dem Markt eine Vielzahl von Aus- und Fortbildungsveranstaltungen angeboten werden, die allein vom zeitlichen Umfang die Mindestqualifikation für Datenschutzbeauftragte nicht vermitteln können. In Anbetracht der steigenden Bedeutung des Datenschutzes in den Unternehmen sind Angebote, die sich auf eine Ausbildung von ein bis drei Tagen beschränken, in aller Regel völlig unzureichend. Das gleiche gilt für die Prüfung der Qualifikation des Datenschutzbeauftragten. Auch hier ist, wie von namhaften Institutionen angeboten, eine einstündige Multiple-Choice-Prüfung nicht hinreichend. Die GDD hat zusammen mit der UDIS gGmbH als führende und erfahrene Ausbildungseinrichtungen ein Konzept hinsichtlich der Mindestanforderungen an die Ausbildung und Prüfung von betrieblichen Datenschutzbeauftragten entwickelt. Dieses kann im Rahmen der Konkretisierung der Anforderungen an die Fachkunde des Datenschutzbeauftragten herangezogen werden.

2. Zu § 28 Abs. 3 BDSG-E (Streichung des Listenprivilegs)

Die Neuregelung sieht eine Streichung des Listenprivilegs für Zwecke des Adresshandels, der Werbung oder der Markt- und Meinungsforschung vor. Die Einschränkung des Listenprivilegs im Hinblick auf die Markt- und Meinungsforschungsinstitute ist nicht angezeigt, da diese Branche durch die aktuellen Datenschutzskandale nicht betroffen war. Im Übrigen werden im Unterschied zum Adresshandel von der Einzelperson unabhängige verallgemeinerungsfähige Aussagen gewonnen und dem Auftraggeber nur in anonymisierter Form übermittelt.

Mit Blick auf die Werbung und den Adresshandel sollen die Rechte des Verbrauchers durch das Einwilligungserfordernis in die Zulässigkeit der listenmäßigen Übermittlung ihrer Daten gestärkt werden. Die Stärkung der informationellen Selbstbestimmung steht im Spannungsverhältnis zum Interesse der Wirtschaft, den eigenen Kundenstamm auch mit Produkten und Dienstleistungen Dritter bewerben zu dürfen.

Ein sinnvoller Kompromiss zwischen der Stärkung der Verbraucherrechte auf der einen und den Interessen der Wirtschaft an einem erfolgreichen Marketing auf der anderen Seite, lässt sich dadurch erreichen, dass eine Nutzung eigener personenbezogener Datenbestände für Werbezwecke Dritter im Rahmen des Listenprivilegs zulässig bleibt. Im Fall dieser Datennutzung kommt es nicht zu einer Übermittlung personenbezogener Daten. Die Daten verbleiben vielmehr in der Herrschaft und der datenschutzrechtlichen Verantwortung des Adresslisteneigners. Dieser versendet lediglich personalisierte Werbung für einen Dritten. Die Transparenz für die Verbraucher bei Nutzung ihrer personenbezogener Daten für Werbezwecke Dritter ist dadurch zu erreichen, dass das für die Datennutzung verantwortliche Unternehmen verpflichtet wird, auf die Datenherrschaft, also auf die Eigenschaft als Absender der Werbebotschaft, hinzuweisen. Im Übrigen ist dem Verbraucher die Nutzung seiner Daten für die Werbung Dritter bekannt, da er bereits bei der Datenerhebung gemäß § 4 Abs. 3 BDSG umfassend über die Zwecke der Datenverarbeitung zu informieren ist. Zugleich besteht weiterhin das Widerspruchsrecht gegen die werbliche Nutzung der Daten nach § 28 Abs. 4 BDSG, der auch eine entsprechende Unterrichtungspflicht vorsieht.

Insbesondere für die Weitergabe von Kundendaten innerhalb eines Konzerns bedarf es jedenfalls nach Einschränkung des Listenprivilegs einer interessengerechten Alternative zum Einwilligungserfordernis. Dem arbeitsteiligen Zusammenwirken kon-

zernangehöriger Unternehmen sollte zumindest über die Zulässigkeit, Werbung im Auftrag eines konzernangehörigen Unternehmens zu versenden, Rechnung getragen werden. Wie oben beschrieben, können durch die Angabe der Adresslisteneignerschaft die Rechte der Betroffen hinreichend gewahrt werden.

Die Transparenz und Kontrolle über die Nutzung eigener personenbezogener Datenbestände für Werbezwecke Dritter kann zusätzlich dadurch gestärkt werden, dass Verfahren für die Ansprache der Verbraucher durch eingeschaltete Dienstleister (z.B. Letter-Shops oder Call-Center), die nach § 11 BDSB als Auftragsdatenverarbeiter tätig werden, nach § 4d Abs. 4 BDSG bei der zuständigen Aufsichtsbehörde zu melden sind. Mittels einer solchen Meldepflicht durch die Dienstleister würde für die Aufsichtsbehörden eine Markttransparenz über die Unternehmen geschaffen, die geschäftsmäßig mit Verbraucherdaten für Werbezwecke Umgang haben. Zugleich hätte der Auftraggeber über den Nachweis der Meldung einen zusätzlichen Indikator für die in § 11 Abs. 2 BDSG geforderte sorgfältige Auswahl des Dienstleisters.

Durch Beibehaltung der Erlaubnis zur Nutzung eigener personenbezogener Datenbestände für Werbezwecke Dritter im Rahmen des Listenprivilegs kann somit das Ziel der Gesetzesinitiative, ein Vagabundieren von Verbraucherdaten zu unterbinden, erreicht werden, ohne legitime wirtschaftliche Interessen an der Datenverwendung übermäßig zu beschneiden.

3. Zu § 28 Abs. 3a BDSG-E (Einwilligung in Übermittlung von Listendaten)

Der Standort der Regelung für die Einwilligung in § 28 BDSG ist systematisch unglücklich. Vielmehr sollte die Einwilligung in die listenmäßige Übermittlung personenbezogener Daten in die allgemeine Regelung zur Einwilligung des § 4a BDSG integriert werden, auch wenn sich die Regelung nur auf den dritten Abschnitt des BDSG bezieht. Der Entwurf des § 28 Abs. 3a BDSG enthält zudem keine Regelung über bereits erteilte Einwilligungen zu Zwecken der Werbung oder Markt- und Meinungsforschung, die die neuen Formvoraussetzungen nicht erfüllen. Die Notwendigkeit einer solchen Formvoraussetzung unterstellt, sollte klargestellt werden, dass bereits bestehende Einwilligungserklärungen ihre Wirksamkeit erhalten und nicht nachgeholt werden müssen.

4. Zu § 42a BDSG-E (Benachrichtigungspflicht bei Datenverlusten)

Unter dem Aspekt der Verhältnismäßigkeit ist im Rahmen der Benachrichtigungspflicht bei Datenverlusten ein zweistufiges Verfahren anzuraten, wonach zunächst nur die Aufsichtsbehörde zu benachrichtigen ist. Diese könnte dann feststellen, ob und ggf. wie die Benachrichtigung der Betroffenen erfolgen sollte. Auch dürfte es für manche Unternehmen unangemessenen sein, in mindestens zwei bundesweit erscheinenden Tageszeitungen großformatige Informationsanzeigen platzieren zu müssen. In Betracht kommt alternativ die Veröffentlichung in einer zielgruppenorientierten Zeitung bzw. Fachzeitschrift oder eine Veröffentlichung über das Internet, z.B. über eine neutrale und bekannte Website wie „datenschutz.de“. Warum die Benachrichtigungspflicht sich ausschließlich auf nicht öffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen beschränken soll, ist zudem nicht nachvollziehbar.

Bonn, den 13. März 2009